(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 199 20 299 A 1**

(51) Int. Cl.[7]:
G 08 B 29/16
H 04 L 1/22

(21) Aktenzeichen: 199 20 299.0
(22) Anmeldetag: 3. 5. 1999
(43) Offenlegungstag: 9. 11. 2000

DE 199 20 299 A 1

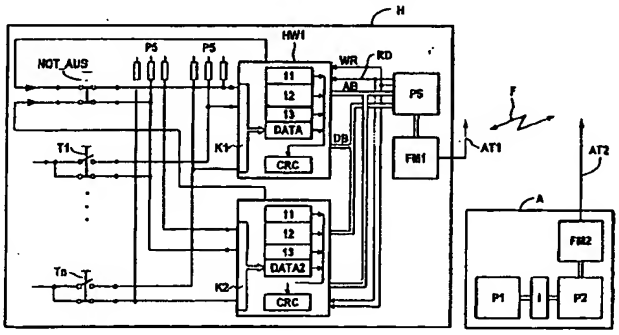
(71) Anmelder:
Siemens AG, 80333 München, DE

(72) Erfinder:
Rumpler, Gerhard, Dipl.-Ing., 91056 Erlangen, DE; Kahle-Nobis, Gerhard, Dipl.-Ing., 90425 Nürnberg, DE; Meier, Christof, Dr.-Ing., 91336 Heroldsbach, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Verfahren sowie Vorrichtung zur Erfassung, Übertragung und Verarbeitung sicherheitsgerichteter Signale

(57) Die Erfindung erlaubt die Anwendung der Funktechnik zur Übertragtung von NOT-AUS-, START-, STOP- sowie Verfahr- und Zustimmungssignalen von industriellen Bearbeitungsmaschinen wie beispielsweise numerisch gesteuerten Werkzeugmaschinen und Robotern über Funk. Auf zusätzliche Sicherungsmaßnahmen von START- und Verfahrenssignalen mittels Zustimmungssignal kann verzichtet werden, sofern die Steuerungsfunktionen entsprechende Sicherheitsanforderungen erfüllen. Dazu werden sicherheitsgerichtete Signale auf Senderseite physikalisch mindestens zweikanalig erfaßt, die erfaßten Daten logisch mindestens zweikanalig in sicherer Technik über Funk übertragen und die empfangenen Daten auf der Empfängerseite ebenfalls physikalisch mindestens zweikanalig verarbeitet und überwacht. Neben den sicherheitsgerichteten Signaldaten werden für Überwachungszwecke zusätzliche Sicherungsdaten erzeugt, mit denen auf Empfängerseite eine Überwachung durch Überprüfung eines Redundanzwertes zur Datensicherung auf Plausibilität sowie kreuzweisen Vergleich der Auswertungsergebnisse etc. vorgenommen wird.



DE 199 20 299 A 1

Beschreibung

Die Erfindung bezieht sich auf ein Verfahren sowie eine Vorrichtung zur Erfassung, Übertragung und Verarbeitung sicherheitsgerichteter Signale mit mindestens einem Erfassungsmittel, einer Übertragungsstrecke und mindestens einem Signalverarbeitungsmittel.

Zum Steuern von Maschinen in Fertigungsanlagen in der Industrie, insbesondere von Werkzeugmaschinen und Robotern, werden Signale von Bediengeräten oder Peripheriegeräten an eine Steuerungseinheit übertragen. Dabei kann es sich bei Bedien- und Peripheriegeräten sowohl um stationäre als auch um mobile Einheiten handeln. Regelmäßig müssen insbesondere sicherheitsrelevante Signale wie NOT-AUS-, NOT-HALT-, START-, STOP-, Zustimmungssignale, Verfahrtasten und sicherheitsgerichtete Eingangssignale zuverlässig erfaßt, übertragen und verarbeitet werden, um die Sicherheit des Bedienpersonals, der Maschinen und Anlagen zu gewährleisten. Auch bewegungsauslösende Signale z. B. Achsverfahren, Greifer-Auf und ähnliches gehören zu dieser Problematik.

Deshalb erfolgt herkömmlicherweise die Übertragung sicherheitsgerichteter Signale im allgemeinen drahtgebunden. Nach dem Stand der Technik erfolgt die Erfassung von NOT-AUS, Zustimmung und sicherheitsrelevanten Eingangssignalen über doppelte elektromechanische Schaltelemente. Die Erfassung von Verfahrtasten, START und STOP hingegen erfolgt über einfache elektromechanische, elektrische oder elektronische Schaltelemente.

Für die Übertragung werden die Signale herkömmlicherweise über ein Bussystem, eine serielle Verbindung oder eine parallele Verbindung oder aber direkt über Leitungen übertragen.

NOT-AUS-Signale werden über zwei Leitungspaare zu sicherheitstechnischen Auslöseeinheiten geführt. Abhängig von der Betriebsart werden an START-, STOP- und Verfahrtasten hingegen unterschiedliche Sicherheitsanforderungen gestellt. Die Übertragung der START-, STOP- und Verfahrtastensignale erfolgt im allgemeinen über das genannte Bussystem, die serielle oder die parallele Verbindung. Ist mit diesen Signalen eine sicherheitstechnische Funktion verbunden, so werden die Signale nur in Zusammenwirkung mit Zustimmtasten wirksam, die über Leitungen zur Auslöseeinheit geführt werden. Solche sogenannte Zustimmtasten sind dabei gleichzeitig mit den Verfahrtasten zu betätigen. Sicherheitsrelevante Eingänge werden über eigene Leitungen geführt.

Die Übertragung selbst erfolgt herkömmlicherweise über ein Kabel, welches neben den notwendigen Signalleitungen üblicherweise auch Versorgungsleitungen für Strom bzw. Spannung für die Bedieneinheit enthält. Das Kabel muß für industrielle Einsatzbedingungen geeignet sein, was bedeutet, daß elektrische Störungen, mechanische Belastungen und chemische Einflüsse berücksichtigt werden müssen.

Die Verarbeitung der Signale wie NOT-AUS- und Zustimmsignalen erfolgt elektrisch zweikanalig. Die Verarbeitung der START-, STOP- und Verfahrtasten erfolgt hingegen einkanalig unter Berücksichtigung eines Zustimmsignals.

Infolge der drahtgebundenen Verbindung zwischen Steuerungseinheit und Bedien- oder Peripheriegeräten ergeben sich als Nachteile insbesondere die Kosten für eine leitungsgebundene Verbindung, der dadurch verbundene Installationsaufwand sowie eine geringere Mobilität, Wartungsaufwand für das Kabel, eine dadurch bedingte Unfallgefahr, sowie die Notwendigkeit der bereits beschriebenen Zustimmtaste.

Aufgabe der vorliegenden Erfindung ist es, ein Verfahren sowie eine Vorrichtung zum Erfassen, Übertragen und Verarbeiten sicherheitsgerichteter Signale zu schaffen, bei denen die im vorangehenden genannten Nachteile vermieden werden können.

Unter sicherheitsgerichteten Signalen werden hierbei solche Signale verstanden, bei welchen Fehler bei der Erfassung, Übertragung und Auswertung zu einem Verlust von Sicherheitsfunktionen der Maschine und Anlage oder des Prozesses führen können.

Gemäß der vorliegenden Erfindung wird diese Aufgabe durch ein Verfahren zur Erfassung, Übertragung und Verarbeitung sicherheitsgerichteter Signale mit mindestens einem Erfassungsmittel, einer Übertragungsstrecke und mindestens einem Signalverarbeitungsmittel dadurch gelöst, daß

- sicherheitsgerichtete Signale auf einer Senderseite physikalisch mindestens zweikanalig erfaßt werden,
- die erfaßten Daten logisch mindestens zweikanalig in sicherer Technik über Funk an eine Empfängerseite übertragen werden und
- die empfangenen Daten auf der Empfängerseite ebenfalls physikalisch mindestens zweikanalig verarbeitet und überwacht werden.

Eine entsprechende Vorrichtung zur Lösung der vorangehenden Aufgabe nach der vorliegenden Erfindung ist dadurch gekennzeichnet, daß

- die Erfassungsmittel für sicherheitsgerichtete Signale auf einer Senderseite physikalisch mindestens zweikanalig ausgestaltet sind,
- eine logisch mindestens zweikanalige Funkstrecke in sicherer Technik mit je einem Funkmodul auf Senderseite und Empfängerseite vorgesehen ist und
- die Signalverarbeitungsmittel auf der Empfängerseite ebenfalls physikalisch mindestens zweikanalig ausgestaltet sind.

Durch die vorliegende Erfindung wird somit eine Funkübertragung von Signalen zur Steuerung von Maschinen, Geräten und Prozessen einschließlich sicherheitsrelevanter Signale wie NOT-AUS, NOT-HALT, START, STOP, Zustimmungssignale, Verfahrtasten und sicherheitsgerichteter Eingangssignale sowie bewegungsauslösende Signale ermöglicht. Auch wird eine sichere Auswertung der genannten Signale durch Software realisierbar. Weiterhin ist gewährleistet, daß ein einzelner Fehler bei der Erfassung, Übertragung und Auswertung nicht zu einem Verlust von Sicherheitsfunktionen führt.

Nach einer ersten vorteilhaften Ausgestaltung erfolgt die Erfassung der sicherheitsgerichteten Signale, indem redundante Signale beispielsweise mittels doppelter elektromechanischer, elektrischer oder elektronischer Eingabeelemente erzeugt werden. Die Erfassung verschiedener redundanter Signale erfolgt zweikanalig durch zwei Erfassungsbausteine und ist entweder in Hardware oder in Hard- und Software realisierbar. Mit den erfaßten Signalen werden von jedem Erfassungsbaustein Sicherungsdaten für die Signalübertragung bereitgestellt, die eine Überwachung ermöglicht auf

- falschen Absender oder falschen Empfänger,
- Verfälschung der Daten,
- Verlust von Daten und
- Wiederholung von Daten.

Dabei werden von jedem Erfassungsmittel aus den Signaldaten für Überwachungszwecke zusätzliche Sicherungsdaten erzeugt.

Die Übertragung erfolgt nach einer weiteren vorteilhaften Ausgestaltung der Erfindung durch einen Sendebaustein, je ein Sende- und Empfangsmodul und einen Empfängerbaustein. Sende- und Empfangsbaustein sowie die Funkmodule bestehen jeweils aus verschiedenen Komponenten. Die Funkübertragung erfolgt in digitaler Technik. Die Signalverarbeitung für die Übertragung kann in wesentlichen Teile in Software realisiert sein. Der Sendebaustein übernimmt zyklisch die Signaldaten und die zugehörigen Sicherungsdaten von beiden Erfassungsbausteinen. Die Daten beider Kanäle werden dann gemeinsam per Funk übertragen. Vom Empfängerbaustein werden die empfangenen Daten beider Kanäle wieder getrennt. Zur Verarbeitung der Daten und zur Ausführung der Überwachungsfunktion erfolgt dann die Weitergabe der Daten an den jeweiligen Auswerte- und Überwachungsbaustein für Kanal 1 und Kanal 2.

Die Überwachung und Verarbeitung der Signale erfolgt nach einer weiteren vorteilhaften Ausgestaltung der Erfindung ebenfalls zweikanalig, insbesondere auf zwei separaten Prozessoren, wie beispielsweise Signalprozessoren. Auf jedem Kanal erfolgt eine Überwachung der Daten nach folgenden Kriterien:

- falscher Absender oder falscher Empfänger,
- Verfälschung der Daten bei der Übertragung,
- Verlust von Daten,
- Wiederholung von Daten und
- Unterbrechung der Daten.

In jedem Kanal erfolgt eine Überwachung eines Zeitkriteriums, was zur Folge hat, daß sicherheitsrelevante Funktionen in der Regel nach einer vorgegebenen Zeitdauer nach Erfassung der Signale ausgelöst werden. Dies wird nach der vorliegenden Erfindung gewährleistet, wenn die Signale immer nach einer vorgegebenen Zeitdauer zur Verarbeitung übertragen werden.

In jedem Kanal erfolgt eine Überwachung der Funktionsfähigkeit eines NOT-AUS- und STOP-Eingabeelementes sowie der zugehörigen Funktion des jeweiligen Erfassungsbausteins durch Zwangsdynamisierung.

Der Fehleraufdeckung erfolgt nach der Auswertung in jedem Kanal durch einen Vergleich der Auswertungsergebnisse.

Die auszulösenden Reaktionen nach Aufdeckung eines Fehlers hängen von verschiedenen Faktoren wie der jeweiligen Anwendung, dem jeweiligen Sicherheitskonzept, der jeweiligen Maschine, Steuerung bzw. Anlage ab.

Weiterhin können etwaige Sicherungsverfahren durch Funkübertragung unabhängig von den beschriebenen Überwachung gegebenenfalls zusätzlich durchgeführt werden.

Die Verarbeitung führt zur Ausführung der durch eingegebene Signale auszulösenden Steuerungsfunktion. Die Ausführung der Steuerungsfunktion kann je nach Sicherheitsanforderung ebenfalls zweikanalig erfolgen. Die zweikanalige Erfassung, die sichere Übertragung und die zweikanalige Überwachung sowie Verarbeitung ermöglichen den Verzicht auf ein zusätzliches Zustimmungssignal – z. B. eine Zustimmungstaste –, wenn die nachfolgenden Steuerungsfunktionen entsprechend in sicherer Technik ausgeführt sind.

Nach einer weiteren vorteilhaften Ausgestaltung der Erfindung wird zusätzlich zu den Signaldaten und Sicherungsdaten ein Redundanzwert zur Datensicherung ergänzt und übertragen. Neben einer Überwachung durch kreuzweisen Datenvergleich beider Kanäle kann die Sicherheit der Übertragung durch eine Plausibilitätsprüfung dieses Redundanzwertes zur Datensicherung weiter gesteigert werden.

Nach einer weiteren vorteilhaften Ausgestaltung des Verfahrens sowie der Vorrichtung nach der vorliegenden Erfindung wird eine weitere Erhöhung der Sicherheit erreicht, indem jedes Datenpaket zusätzlich mit einem Zählerwert versehen wird, welcher auf Senderseite erzeugt wird, wobei der Zählerwert für jedes zu übertragende Datenpaket inkrementiert oder dekrementiert wird und der Redundanzwert zur Datensicherung über Signaldaten, Sicherungsdaten und Zählerwert gebildet wird.

Nach einer weiteren vorteilhaften Ausgestaltung des Verfahrens sowie der Vorrichtung gemäß der vorliegenden Erfindung erfolgt eine besonders effiziente Funkübertragung der Daten, indem

- auf der Senderseite jedes Datenpaket in einen impliziten und einen expliziten Datenteil getrennt wird, wobei der implizite Datenteil solche Daten umfaßt, die auf Empfängerseite bekannt sind, und
- zur Minimierung des zu übertragenden Datenvolumens nur der explizite Teil des Datenpakets per Funk übertragen wird und
- auf der Empfängerseite das Datenpaket aus den bekannten Informationen und dem empfangenen expliziten Teil rekonstruiert wird.

Besonders vorteilhaft kann die Erfindung in der Verbindung mit industriellen Bearbeitungsmaschinen oder Fertigungsanlagen, insbesondere numerisch gesteuerten Werkzeugmaschinen oder Robotern, eingesetzt werden.

Dabei ist neben einer Ausgestaltung in zweikanaliger Technik selbstverständlich auch eine Realisierung mit mehr als zwei Kanälen ebenfalls nach der Lehre gemäß der vorliegenden Erfindung möglich.

Der Aufbau einer sicheren Funkdatenverbindung nach der vorliegenden Erfindung läßt sich besonders vorteilhaft durch ein Verfahren realisieren, welches sich dadurch auszeichnet, daß ein Empfänger beim Sender angemeldet wird, indem

- Kommunikationsadressen für Senderseite und Empfängerseite für jeden Kanal eindeutig festgelegt werden,
- eine Funkverbindung zwischen Sender und Empfänger hergestellt wird,
- die Kommunikationsadressen zum Empfänger in Form eines Datenpakets übertragen werden, wobei der Anmeldevorgang abgebrochen wird,
- wenn eine vorgegebenes Zeitfenster überschritten wird oder
- ein Verlust oder eine Wiederholung von Daten auftritt oder
- ein kreuzweiser Vergleich zur Aufdeckung eines Fehlers führt oder
- keine Plausibilität des Redundanzwertes zur Datensicherung erkannt wird.

Aus dem Einsatz des Funksystems zur Übertragung von sicherheitsgerichteten Signalen zur Steuerung von u. a. Maschinen nach der vorliegenden Erfindung ergeben sich somit folgende Vorteile:

- keine Kosten für eine leitungsgebundene Verbindung,
- bei stationären Geräten ein geringerer Installationsaufwand, da keine drahtgebundene Verbindung installiert werden muß,
- bei portablen Geräten eine größere Mobilität, keine Gewichtsbelastung durch ein Kabel, keine Unfallgefahr durch ein Kabel, kein Wartungsaufwand für ein

Kabel und es entfällt der Aufwand für Zustimmungstaster.

Die Erfindung erlaubt somit die Anwendung der Funktechnik zur Übertragung von NOT-AUS-, START-, STOP- sowie Verfahr- und Zustimmungssignalen über Funk. Auf zusätzliche Sicherung von START- und Verfahrsignalen mittels Zustimmungssignalen – insbesondere Zustimmungstastern – kann verzichtet werden, sofern die Steuerungsfunktionen entsprechende Sicherheitsanforderungen erfüllen.

Weitere Vorteile und Details der vorliegenden Erfindung ergeben sich anhand der folgenden Darstellung eines vorteilhaften Ausführungsbeispiels und in Verbindung mit den Figuren. In den Figuren sind Elemente mit gleicher Funktionalität der besseren Übersichtlichkeit halber mit gleichen Bezugszeichen gekennzeichnet. Es zeigen:

Fig. 1 ein Blockschaltbild einer Vorrichtung gemäß der vorliegenden Erfindung,

Fig. 2 eine Datenstruktur eines Datenpakets,

Fig. 3 eine Datenstruktur eines Funktelegramms mit zwei logischen Verbindungen und

Fig. 4 ein Blockschaltbild eines Automatisierungssystems mit einem Handgerät gemäß der vorliegenden Erfindung.

In der Darstellung gemäß **Fig. 1** ist ein stark abstrahiertes Blockschaltbild einer Vorrichtung gezeigt, die in der Darstellung nach **Fig. 4** mit einem höheren Detailierungsgrad beschrieben ist. Nach **Fig. 1** sind auf der linken Seite Eingabemittel schematisch skizziert, die mit einer erster und zweiten Erfassungseinheit EM1 und EM2 verbunden sind. Dem Erfassungsmittel EM1 ist ein erster Kanal K1 zugeordnet, über den die Ausgangssignale zu einem Sendebaustein S geführt werden. Das gleiche geschieht mit den Ausgangssignalen des Erfassungsmittels EM2 über einen Kanal K2. Der Sendebaustein S wiederum steuert ein Funkmodul FM1 an, welches über eine Funkverbindung F Daten an ein zweites Funkmodul FM2 sendet bzw. umgekehrt von diesem empfängt. Über das zweite Funkmodul FM2 gelangen die Daten zu einem Empfängerbaustein E, indem sie auf die senderseitig bereits existierenden Kanäle K1 und K2 aufgetrennt werden und über jeden Kanal einem zugeordneten Verarbeitungsmittel VM1 bzw. VM2 zugeführt werden, über welche dann entsprechende Steuerungsfunktionen ausgelöst werden. Solche Steuerungsfunktionen sind schematisch auf der rechten Seite angedeutet.

Die Darstellung nach **Fig. 4** zeigt ein Blockschaltbild mit einem Handgerät H und einem Automatisierungssystem A, welches zwei unabhängige Empfangsprozessoren P1 und P2 für eine Datenübertragung von sicherheitsrelevanten Tasten (NOT-AUS-, START-, STOP-, Verfahrtasten etc.) über Funk realisiert. Als Funktechnik kann z. B. der digitale Datenfunk nach dem Funkstandard DECT (Digital enhanced cordless telecommunication) realisert werden. Neben den sicherheitsrelevanten Tasten NOT_AUS, T1 ... Tn besitzt das Handgerät H eine zusätzliche sicherheitsrelevante Taste für die Inbetriebnahme und für die Initialisierung der Funkverbindung eine Funkanmeldetaste (nicht gezeigt). Die Steuerung A ist mit einem Funkaktivierungstaster oder -schalter ausgestattet (ebenfalls nicht gezeigt), welcher in sicherer Technik realisiert ist.

Jede sicherheitsrelevante Taste besitzt zwei Schaltkontakte C, D bzw. C1, D1. Bei START- oder Verfahrtasten liefern die Schaltkontakte zwei invertierte Signale. Ist der Taster nicht betätigt, liefert der eine Kontakt einen High-Pegel, der andere einen Low-Pegel. NOT-AUS und STOP liefern zwei gleichgerichtete Signale, indem beide Kontakte als Öffner ausgeführt sind. In der in der Darstellung nach **Fig. 4** beschriebenen Ausführungsform wird der geschlossene Schalterzustand beispielhaft durch Low-Pegel signalisiert. Die zwei Schaltkontakte jedes Schaltelementes NOT_AUS, T1 ... Tn werden jeweils an einen Hardwarebaustein HW1 bzw. HW2 geführt. Jeder Hardwarebaustein setzt die Signalpegel in binäre Daten um. Low zu 0 (NULL) und High zu 1 (EINS). Die Daten werden dann als Tasteninformationen in einem Register DATA für die Übertragung zur Verfügung gestellt. Zusätzlich werden in weiteren Registern **11** bis **23** zur Verfügung gestellt:

- Sendeadresse (Sendeprozessor PS) oder Empfängeradresse (Empfangsprozessor P1 bzw. Empfangsprozessor P2) **12** bzw. **22**, Zählerwert **13** bzw. **23**,
- Redundanzwert zur Datensicherung CRC bzw. CRC2 und
- Länge dieser Daten **11** bzw. **12**.

In den Hardwarebausteinen HW1 bzw. HW2 wird bei jedem Lesezugriff ein Zähler-Wert inkrementiert und ein Hardware-Redundanzcheck durch CRC-Bildung über die Länge, Sendeadresse, Empfängeradresse, Zählerwert und Tasteninformation durchgeführt (CRC bedeutet Cyclic Redundancy Check, ein dem Fachmann bekanntes Verfahren). Beim Zähler handelt es sich beispielsweise um einen Hardware-Zähler, der bei Verbindungsaufbau mit einem Anfangswert geladen wird. Bei jedem Lesezugriff auf die sicherheitsgerichtete Tasteninformation wird dieser Wert inkrementiert (selbstverständlich ist auch eine ständige Dekrementierung möglich) und der Wert über die Funkstrecke übertragen. Durch den gegenüber der letzten sicherheitsgerichteten Information inkrementierten Zählerwert wird auf den Empfängerprozessoren P1 bzw. P2 die Authentizität der Kanalinformation bestätigt.

Vom Sendeprozessor PS werden die Daten beider Hardwarebausteine HW1 und HW2 in einem fest eingestellten Zyklus (z. B. alle 30 msec) ausgelesen und in einem Datenpaket zusammengesfaßt. Der Sendeprozessor übergibt dieses Datenpaket an das erste Funkmodul FM1 zur Übertragung über die Funkstrecke F.

Auf der Empfängerseite werden die Daten vom Funkmodul FM2 über die entsprechende Antenne AT2 empfangen und an – hier beispielhaft – Empfangsprozessor P2 übertragen. Der Empfangsprozessor P2 führt die Überwachung der Daten für Kanal K2 durch. Die Daten für Kanal K1 werden an den Empfangsprozessor P1 übergeben und von diesem überwacht.

In der Darstellung nach **Fig. 2** ist die Datenstruktur eines solchen Datenpaketes skizziert. Die Daten beider Kanäle K1 und K2 werden in einem Datenpaket zusammengefaßt und dieses über einen Funkkanal wie oben geschildert übertragen. Daten eines Übertragungskanals stellen damit eine logische Verbindung dar. Das Datenpaket wird dazu in einen implizierten Teil IM_T und einem expliziten Teil EX_T aufgeteilt. Der implizierte Teil IM_T enthält die Informationen zur Länge **1**, Empfangsadresse **2**, Sendeadresse **3** und den höherwertigen Teil MSB des Zählers **4**. Der explizite Teil EX_T enthält den niederwertigen Teil LSB des Zählers **5**, die Tasteninformation **6** und den Redundanzwert CRC. Die Darstellung nach **Fig. 2** stellt somit die Daten eines Übertragungskanals K1 oder K2 und damit eine logische Verbindung dar. Um die Anzahl der zu senden Daten zu minimieren, werden die Daten des impliziten Teils IM_T nicht übertragen, da diese Daten in den Empfängerprozessoren P1 bzw. P2 hinterlegt und damit bekannt sind.

Dabei dient die Empfängeradresse der eindeutigen Empfängeridentifikation bei Auswertung der übertragenen Struktur im Empfangsprozessor P1 bzw. Empfangsprozes-

sor P2. Die Sendeadresse dient der eindeutigen Senderidentifikation bei Auswertung der übertragenen Struktur im Empfangsprozessor P1 bzw. P2. Der Zähler wurde bereits im vorangehenden erläutert. Der höherwertige Teil MSB des Zählers wird durch Zählerüberläufe auf den Empfängerprozessoren P1 bzw. P2 ermittelt, der vollständige Zählerwert wird aus höherwertigem Teil MSB und niederwertigem Teil LSB zurückgewonnen. Die Tasteninformation stellt den EIN/AUS-Zustand der Tastenschaltkontakte dar. Der Redundanzwert CRC wird aus den Elementen Länge, Empfängeradresse, Sendeadresse, Zählerwert und der Tasteninformation gebildet. Als CRC-Polynom wird beispielsweise ein irreduzibles, primitives Polynom verwendet.

Über die Funkstrecke wird der explizite Teil EX_T der obenbeschriebenen Struktur übertragen. Diese Daten beider Kanäle K1 und K2 finden sich in den Nutzdaten des Funk-Telegramms als zwei logische Verbindungen wieder, deren Datenabfolge schematisch in der Darstellung nach **Fig. 3** gezeigt ist. Zusammen mit der nicht sicherheitsrelevanten Information, die zwischen Handgerät H und Automatisierungssystem A ausgetauscht werden soll, hat ein Funk-Telegramm beispielsweise folgenden Aufbau:

Auf ein Funkprotokoll FP folgt der explizite Teil für Kanal 1 EX_K1, darauf der explizite Teil für Kanal 2 EX_K2 und darauf die nicht sicherheitsrelevanten Daten. Nach diesem Nutzdaten-Funk folgt wiederum ein Funk-Protokoll FP usw.

Bevor eine sichere Kommunikation aufgebaut werden kann, muß das Handgerät bei der Steuerung angemeldet werden. Diese Anmeldung muß für jedes Kommunikationspaar (Handgerät/Steuerung) einmalig durchgeführt werden.

Bei der Anmeldung werden die Kommunikationsadressen für Handgerät und Automatisierungsgerät eindeutig festgelegt: Für Handgerät und Automatisierungsgerät wird jeweils je Kanal eine Sender- bzw. Empfängeradresse festgelegt. Pro Verbindung werden also vier Adressen benötigt. Es besteht dadurch eine eindeutige Zuordnung zwischen Handgerät und Steuerung, die auch durch Anzeigen bzw. durch eine festaufgebrachte Kennzeichnung signalisiert werden kann. Das Verfahren dieser Adressenvergabe ist im folgenden beschrieben:

Für die Anmeldung erfolgen Bedienhandlungen an folgenden Bedienelementen:
an der Steuerung:

- Funkaktivierungsschalter (z. B. Schlüsselschalter) mit folgenden Stellungen
- 0 AUS
- 1 Anmelden
- 2 Sichere Funkkommunikation

am Handerät

- Funk-Ein-Aus-Taster.

Die Anmeldung muß innerhalb einer fest vorgegebenen Zeit durchgeführt werden (z. B. 60 Sekunden).

1. Funkaktivierungsschalter in Stellung "Anmelden" bringen und Handgerät einschalten, dadurch erfolgt der Aufbau der Funkverbindung. Dieser Vorgang kann durch Eingeben eines Passworts und Sicherheitscodes für Maschine und Handgerät vor Mißbrauch oder versehentlicher Ausführung geschützt werden.
2. Für das Anmeldeverfahren sind die Adressen von Sender und Empfänger immer gleich (siehe unten). Die verwendeten Adreßwerte 01h und Feh sind bei der späteren Adreßbestimmung ausgeschlossen. Vom Handgerät werden eine fest vorgegebene Anzahl von Anmelde-Datenblöcken (z. B. 200) gesendet. Die Anmelde-Datenblöcke sind gemäß der oben beschriebenen Datenstruktur (**Fig. 2**) beispielhaft mit folgenden Werten aufgebaut:
   - Sender 1 = Feh
   - Sender 2 = 01h
   - Empfänger 1 = 01h
   - Empfänger 2 = Feh
   - Zählerwert = F000 0000h

   Von beiden Empfängerprozessoren erfolgt eine Überwachung nach allen weiter unten beschriebenen Kriterien. Jeder erkannte Fehler führt zum Abbruch der Anmeldung.
3. Während Anmelde-Datenblöcke gesendet werden, ist am Handgerät die Funk-Ein-Aus-Taste (sicherheitsrelevant) für eine begrenzte Zeit (z. B. 1 Sekunde) zu betätigen. Während dieser Zeit ist an der Steuerung der Funkaktivierungsschalter in Stellung 2 zu bringen.
4. Ausgelöst durch den Funkaktivierungsschalter werden von einem Empfangsprozessor nacheinander vier Zufallszahlen generiert und an das Handgerät übermittelt. Für die Zahlen gilt: 01H < Zufallszahl < Feh, d. h. die Werte 0, 1, 254 und 255 sind ausgeschlossen.
5. Vom Handgerät wird dann eine fest vorgegebene Anzahl von Datenblöcken (z. B. 2 Datenblöcke) gesendet, wobei im ersten Datenblock der erste Zufallswert als Senderadresse 1 angenommen wird und dieser erste Zufallswert gleichzeitig im expliziten Teil als Zählerwert übermittelt wird. In weiteren Datenblöcken wird dieser Zählerwert inkrementiert.
6. Vom Handgerät wird dann eine fest vorgegebene Anzahl von Datenblöcken (z. B. 2 Datenblöcke) gesendet, wobei im ersten Datenblock der zweite Zufallswert als Senderadresse 2 angenommen wird und dieser zweite Zufallswert gleichzeitig im expliziten Teil als Zählerwert übermittelt wird. In weiteren Datenblöcken wird dieser Zählerwert inkrementiert.
7. In der gleichen Weise werden die Empfängeradressen in weiteren Datenblöcken an die Empfängerprozessoren zurückübermittelt.
8. Vom Handgerät werden dann Datenblöcke mit dem folgenden Aufbau gesendet:
   - Sender 1 wie festgelegt
     Sender 2 wie festgelegt
   - Empfänger 1 wie festgelegt
   - Empfänger 2 wie festgelegt

   Als erster Zählerwert ist festgelegt:
   - Zählerwert = der fortlaufend inkrementierte zuletzt eingetragene Wert.

   Von beiden Empfängerprozessoren erfolgt eine Überwachung nach allen weiter unten beschriebenen Kriterien. Jeder erkannte Fehler führt zum Abbruch der Initialisierung.
9. Nun muß die Anmeldung durch folgende Bedienhandlung beendet werden: Am Handgerät ist die Funk-Ein-Aus-Taste (sicherheitsrelevant) für eine begrenzte Zeit (z. B. 1 Sekunde) zu betätigen. Während dieser Zeit ist an der Steuerung der Funkaktivierungsschalter in die Stellung 0 zu bringen.

Von beiden Empfängerprozessoren erfolgt bei allen Datenblöcken eine Überwachung nach allen weiter unten beschriebenen Kriterien. Jeder erkannte Fehler führt zum Abbruch der Anmeldung. Ausnahmen sind die Schritte 5 bis 7. Die Änderung der impliziten Adressen erkennen die Empfängerprozessoren anhand eines Fehlers bei der CRC-Überprüfung. Hier wird dann erwartet, daß der jeweils folgende

Datenblock allen Überwachungskriterien wieder genügt.

Zusätzlich wird von den Empfängerprozessoren überwacht, daß das ganze Anmeldungsverfahren innerhalb der obengenannten fest vorgegebenen Zeit abgeschlossen wird. Sonst erfolgt ebenfalls ein Abbruch.

Damit sind die zum Aufbau einer sicheren Verbindung benötigten Adressen zwischen Sender und Empfänger eindeutig festgelegt.

Zur Initialisierung der Kommunikation:

Zum Aufbau einer sicheren Verbindung muß die folgende Initialisierung durchgeführt werden.

1. Durch eine Bedienhandlung am Handgerät (Auswahl der Maschine) wird die Funk-Verbindung aufgebaut. Vom Handgerät werden Datenblöcke gemäß der oben beschriebenen Datenstruktur mit folgenden Daten gesendet:
   - Sender 1 wie bei Anmeldung festgelegt
   - Sender 2 wie bei Anmeldung festgelegt
   - Empfänger 1 wie bei Anmeldung festgelegt
   - Empfänger 2 wie bei Anmeldung festgelegt
   - Zählerwert = 0000 0000h

   Von beiden Empfängerprozessoren erfolgt eine Überwachung nach allen weiter unten beschriebenen Kriterien. Jeder erkannte Fehler führt zum Abbruch der Initialisierung.
2. Innerhalb einer fest vorgegebenen Zeit (z. B. 60 Sekunden) ist am Handgerät die Funk-Ein-Aus-Taste (sicherheitsrelevant) für eine begrenzte Zeit (z. B. 1 Sekunde) zu betätigen. Während dieser Zeit ist an der Steuerung der Funkaktivierungsschalter in Stellung 2 zu bringen. Damit ist die sichere Verbindung aufgebaut.

Von beiden Empfängerprozessoren erfolgt eine Überwachung nach allen weiter unten beschriebenen Kriterien. Jeder erkannte Fehler führt zum Abbruch der Initialisierung.

Zum Abbau der Kommunikation:

Der gezielte Abbau der Verbindung erfolgt durch abermalige Betätigung der Funk-Ein-Aus-Taste am Handgerät und Ausschalten am Funkaktivierungsschalter (Stellung 0).

Überwachung und Auswertung der Daten auf Empfängerseite:

Auf der Empfängerseite erfolgt die Überwachung und Bearbeitung der Daten auf zwei unabhängigen Prozessoren (Empfangsprozessor 1 und Empfangsprozessor 2) in gleicher Weise.

Plausibilitätsüberprüfung der Längenangabe:

Die Längenangabe wird nicht übertragen, sondern ist Bestandteil des impliziten Teils der Daten. Der Wert ist, wie oben beschrieben, fest vorgegeben. Die Ermittlung der Position der Daten, des Zählerwertes und des CRC-Wertes im expliziten Teil der Daten erfolgt mit Hilfe des vorgegebenen Längenwertes. Die Richtigkeit der ausgelesenen Werte hängt also von der Richtigkeit des Längenwertes ab. Durch die im folgenden beschriebene Überprüfung der übertragenen Werte erfolgt also gleichzeitig eine Überprüfung des Längenwertes.

Überprüfung auf Verfälschung der Daten:

Die Überprüfung auf Verfälschung der Daten erfolgt mittels des übertragenen CRC-Anhangs. Auf der Empfängerseite wird aus den impliziten Daten

- Länge
- Empfängeradresse
- Senderadresse
- Zählerwert (3 MSB)

und den übertragenen expliziten Daten

- Zählerwert (1 LSB)
- Sichere-Tastensignale

ein CRC-Vergleichswert bestimmt (wie oben beschrieben). Dieser wird mit dem übertragenen CRC-Wert verglichen.

Überprüfung von Sender- und Empfängeradresse:

Empfänger- und Absenderadressen werden nicht übertragen, gehen aber in die CRC-Bestimmung ein. Deshalb ist die oben beschriebene Überprüfung auf Verfälschung der Daten gleichzeitig eine Überprüfung der richtigen Sender- und Empfängeradressen.

Überprüfung auf Verlust und Wiederholung von Daten:

Durch Vergleich des Zählerwertes des aktuellen Datenpaktes mit dem Zählerwert des vorherigen Datenpaktes, wird die Aufeinanderfolge von Datenpakten ermittelt und damit ein Verlust oder eine Wiederholung von Datenpaketen erkannt.

Überprüfung auf Übertragungsstörung:

Eine Unterbrechung der Funkverbindung bzw. der gesamten Kommunikationsstrecke wird durch eine Lebenszeichenüberwachung realisiert. Es wird erwartet, daß regelmäßig Datenpakte empfangen werden. Für den maximalen zeitlichen Abstand zweier aufeinanderfolgender Pakete wird eine Zeitdauer festgelegt. Wird diese Zeit überschritten, so gilt die Übertragung als gestört.

Kreuzweiser Vergleich:

Zur weiteren Fehleraufdeckung wird zwischen beiden Kanälen ein kreuzweiser Datenvergleich durchgeführt.

Wird nach den obengenannten Kriterien ein Fehler erkannt, so erfolgt kein Aufbau der Verbindung. Wird kein Fehler erkannt, so gilt die Verbindung als sicher und es erfolgt eine erste Auswertung der Signal- bzw. Tastendaten.

Patentansprüche

1. Verfahren zur Erfassung, Übertragung und Verarbeitung sicherheitsgerichteter Signale mit mindestens einem Erfassungsmittel (EM1, EM2), einer Übertragungsstrecke (FM1, F, FM2) und mindestens einem Signalverarbeitungsmittel (VM1, VM2), **dadurch gekennzeichnet**, daß
   - sicherheitsgerichtete Signale auf einer Senderseite (S) physikalisch mindestens zweikanalig (K1, K2) erfaßt (EM1, EM2) werden,
   - die erfaßten Daten logisch mindestens zweikanalig in sicherer Technik über Funk (FM1, F, FM2) an eine Empfängerseite (E) übertragen werden und
   - die empfangenen Daten auf der Empängerseite (E) ebenfalls physikalisch mindestens zweikanalig (K1, K2) verarbeitet (VM1, VM2) und überwacht werden.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß zur mindestens zweikanaligen Verarbeitung als Signaldaten redundante Signale mittels mindestens doppelter elektromechanischer, elektrischer oder elektronischer Eingabeelemente (T1, Tn, NOT_AUS) erzeugt werden und von jedem Erfassungsmittel (EM1, EM2) aus den Signaldaten für Überwachungszwecke zusätzliche Sicherungsdaten erzeugt werden, die eine Überwachung ermöglichen auf
   - falschen Sender oder falschen Empfänger und/oder
   - Verfälschung der sicherheitsgerichteten Daten und/oder
   - Verlust von Daten und/oder

– Wiederholung von Daten.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die Funkübertragung in digitaler Technik erfolgt, wobei

– Signaldaten und Sicherungsdaten zyklisch erfaßt werden,
– ein Datenpaket aus den Signaldaten und Sicherungsdaten beider Kanäle (K1, K2) gebildet wird, welches durch einen Redundanzwert zur Datensicherung (CRC) ergänzt wird, und
– dieses Datenpaket per Funk zur Empfängerseite übertragen wird.

4. Verfahren nach Anspruch 1 oder 2 oder 3, dadurch gekennzeichnet, daß auf Empfängerseite für jedes empfangene Datenpaket die

– Signaldaten und Sicherungsdaten beider Kanäle (K1, K2) wieder getrennt werden,
– eine Überprüfung des Redundanzwertes zur Datensicherung (CRC) auf Plausibilität erfolgt,
– in jedem Kanal (K1, K2) ein Vergleich der Auswertungsergebnisse erfolgt und
– bei Korrektheit der Auswertung die empfangenen Signaldaten und Sicherungsdaten für den jeweils zugeordneten Kanal (K1, K2) zur Verarbeitung der sicherheitsgerichteten Daten und zu Überwachungszwecken an die zugeordneten Signalverarbeitungsmittel (VM1, VM2) weitergeleitet werden.

5. Verfahren nach einem der Ansprüche 2 bis 4, dadurch gekennzeichnet, daß auf der Empfängerseite in jedem Kanal die empfangenen Signaldaten und Sicherungsdaten überwacht werden auf

– falschen Sender oder falschen Empfänger und/oder
Verfälschung der sicherheitsgerichteten Daten und/oder
– Verlust von Daten und/oder
– Wiederholung von Daten und/oder
– Unterbrechung der Übertragung.

6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, daß in jedem Kanal (K1, K2) die Funktionsfähigkeit von Not-Aus- oder Stop-Eingabemitteln (NOT_AUS) und der zugehörigen Funktion der Erfassungsmittel (EM1, EM2) durch eine Zwangsdynamisierung überwacht werden.

7. Verfahren nach einem der Ansprüche 3 bis 6, dadurch gekennzeichnet, daß jedes Datenpaket zusätzlich mit einem Zählerwert versehen wird, welcher auf Senderseite erzeugt wird, wobei der Zählerwert für jedes zu übertragende Datenpaket inkrementiert oder dekrementiert wird und der Redundanzwert zur Datensicherung (CRC) über Signaldaten, Sicherungsdaten und Zählerwert gebildet wird.

8. Verfahren nach einem der Ansprüche 3 bis 7, dadurch gekennzeichnet, daß

– auf der Senderseite jedes Datenpaket in einen impliziten (IM_T) und einen expliziten (EX_T) Datenteil getrennt wird, wobei der implizite Datenteil (IM_T) solche Daten umfaßt, die auf Empfängerseite bekannt sind, und
– zur Minimierung des zu übertragenden Datenvolumens nur der explizite Teil (EX_T) des Datenpakets per Funk übertragen wird und
– auf der Empfängerseite das Datenpaket aus den bekannten Informationen und dem empfangenen expliziten Teil (EX_T) rekonstruiert wird.

9. Verfahren zum Aufbau einer sicheren Funkdatenverbindung nach einem der vorangehenden Ansprüche 3 bis 8, dadurch gekennzeichnet, daß ein Empfänger (E) beim Sender (S) angemeldet wird, indem

– Kommunikationsadressen für Senderseite und Empfängerseite für jeden Kanal (K1, K2) eindeutig festgelegt werden,
– eine Funkverbindung zwischen Sender (S) und Empfänger (E) hergestellt wird,
– die Kommunikationsadressen zum Empfänger (E) in Form eines Datenpakets übertragen werden, wobei der Anmeldevorgang abgebrochen wird,
– wenn eine vorgegebenes Zeitfenster überschritten wird oder
– ein Verlust oder eine Wiederholung von Daten auftritt oder
– ein kreuzweiser Vergleich zur Aufdeckung eines Fehlers führt oder
– keine Plausibilität des Redundanzwertes zur Datensicherung (CRC) erkannt wird.

10. Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß als sicherheitsgerichtete Signale Not-Aus und/oder Not-Halt und/oder bewegungsauslösende Signale und/oder Zustimmungssignale für Steuerungszwecke in der Industrieautomatisierung vorgesehen sind.

11. Vorrichtung zur Erfassung, Übertragung und Verarbeitung sicherheitsgerichteter Signale mit mindestens einem Erfassungsmittel (EM1, EM2), einer Übertragungsstrecke (FM1, F, FM2) und mindestens einem Signalverarbeitungsmittel (VM1, VM2), dadurch gekennzeichnet, daß

– die Erfassungsmittel (EM1, EM2) für sicherheitsgerichtete Signale auf einer Senderseite (S) physikalisch mindestens zweikanalig (K1, K2) ausgestaltet sind,
eine logisch mindestens zweikanalige Funkstrecke (F) in sicherer Technik mit je einem Funkmodul (FM1, FM2) auf Senderseite (5) und Empfängerseite (E) vorgesehen ist und
– die Signalverarbeitungsmittel (VM1, VM2) auf der Empängerseite (E) ebenfalls physikalisch mindestens zweikanalig (K1, K2) ausgestaltet sind.

12. Vorrichtung nach Anspruch 11, dadurch gekennzeichnet, daß zur Erzeugung redundanter Signale mindestens doppelte elektromechanische, elektrische oder elektronische Eingabeelemente (T1, Tn, NOT_AUS) vorgesehen sind und die Erfassungsmittel (EM1, EM2) so ausgestaltet sind, daß aus den Signaldaten für Überwachungszwecke zusätzliche Sicherungsdaten erzeugbar sind, die eine Überwachung ermöglichen auf

– falschen Sender oder falschen Empfänger und/oder
– Verfälschung der sicherheitsgerichteten Daten und/oder
– Verlust von Daten und/oder
– Wiederholung von Daten.

13. Vorrichtung nach Anspruch 11 oder 12, dadurch gekennzeichnet, daß die Funkübertragung in digitaler Technik erfolgt, wobei

durch die Erfassungsmittel (EM1, EM2) die Signaldaten und Sicherungsdaten zyklisch erfaßbar sind,
– ein Sendebaustein (PS) vorgesehen ist, durch den ein Datenpaket aus den Signaldaten und Sicherungsdaten beider Kanäle (K1, K2) gebildet wird, welches durch einen Redundanzwert zur Datensicherung (CRC) ergänzt wird, und
– dieses Datenpaket per Funk zur Empfängerseite

übertragen wird.

14. Vorrichtung nach Anspruch 11 oder 12 oder 13, dadurch gekennzeichnet, daß auf Empfängerseite mindestens zwei Empfängerbausteine (P1, P2) vorgesehen sind, durch die für jedes empfangene Datenpaket die
- Signaldaten und Sicherungsdaten beider Kanäle (K1, K2) wieder getrennt werden,
- eine Überprüfung des Redundanzwertes zur Datensicherung (CRC) auf Plausibilität erfolgt,
- in jedem Kanal (K1, K2) ein Vergleich der Auswertungsergebnisse erfolgt und
- bei Korrektheit der Auswertung die empfangenen Signaldaten und Sicherungsdaten für den jeweils zugeordneten Kanal (K1, K2) zur Verarbeitung der sicherheitsgerichteten Daten und zu Überwachungszwecken an die zugeordneten Signalverarbeitungsmittel (VM1, VM2) weitergeleitet werden.

15. Vorrichtung nach einem der Ansprüche 12 bis 14, dadurch gekennzeichnet, daß auf der Empfängerseite Überwachungsmittel vorgesehen sind, mit denen in jedem Kanal die empfangenen Signaldaten und Sicherungsdaten überwachbar sind auf
- falschen Sender oder falschen Empfänger und/oder
- Verfälschung der sicherheitsgerichteten Daten und/oder
- Verlust von Daten und/oder
- Wiederholung von Daten und/oder
- Unterbrechung der Übertragung.

16. Vorrichtung nach Anspruch 15, dadurch gekennzeichnet, daß die Empfängerbausteine (P1, P2 auch die Funktion der Überwachungsmittel übernehmen.

17. Vorrichtung nach einem der Ansprüche 11 bis 16, dadurch gekennzeichnet, daß in jedem Kanal (K1, K2) die Funktionsfähigkeit von Not-Aus- oder Stop-Eingabemitteln (NOT_AUS) und der zugehörigen Funktion der Erfassungsmittel (EM1, EM2) durch Mittel zur Zwangsdynamisierung überwacht werden.

18. Vorrichtung nach einem der Ansprüche 13 bis 17, dadurch gekennzeichnet, daß jedes Datenpaket zusätzlich mit einem Zählerwert versehen wird, welcher auf Senderseite erzeugt wird, wobei der Zählerwert für jedes zu übertragende Datenpaket inkrementiert oder dekrementiert wird und der Redundanzwert zur Datensicherung (CRC) über Signaldaten, Sicherungsdaten und Zählerwert gebildet wird.

19. Vorrichtung nach einem der Ansprüche 13 bis 18, dadurch gekennzeichnet, daß
- durch den Sendebaustein (PS) jedes Datenpaket in einen impliziten (IM_T) und einen expliziten (EX_T) Datenteil getrennt wird, wobei der implizite Datenteil (IM_T) solche Daten umfaßt, die auf Empfängerseite bekannt sind, und
- zur Minimierung des zu übertragenden Datenvolumens nur der explizite Teil (EX_T) des Datenpakets per Funk übertragen wird und
- durch mindestens einen der Empfängerbausteine (P1, P2) das Datenpaket aus den bekannten Informationen und dem empfangenen expliziten Teil (EX_T) rekonstruiert wird.

20. Industrielle Bearbeitungsmaschine oder Fertigungsanlage mit einer Vorrichtung nach einem der Ansprüche 11 bis 19, insbesondere eine numerisch gesteuerte Werkzeugmaschine oder ein Roboter.

Hierzu 2 Seite(n) Zeichnungen

Nummer: DE 199 20 299 A1
Int. Cl.[7]: G 08 B 29/16
Offenlegungstag: 9. November 2000

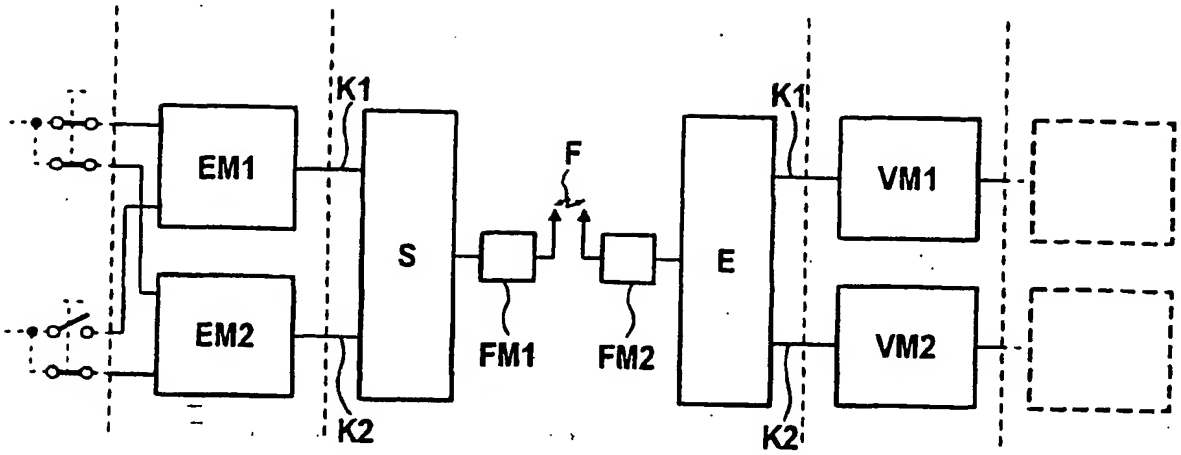


FIG 1

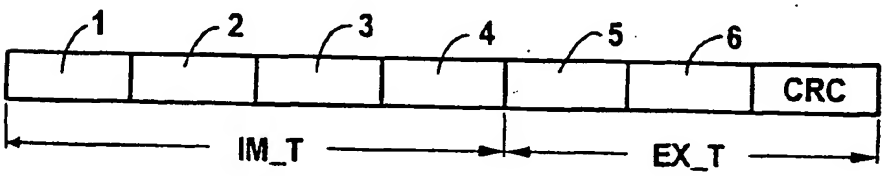


FIG 2

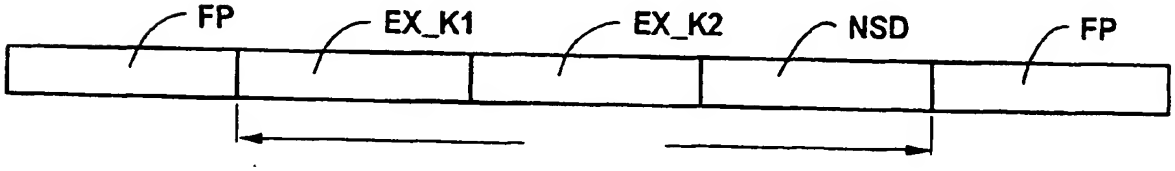


FIG 3

Nummer: DE 199 20 299 A1
Int. Cl.[7]: G 08 B 29/16
Offenlegungstag: 9. November 2000

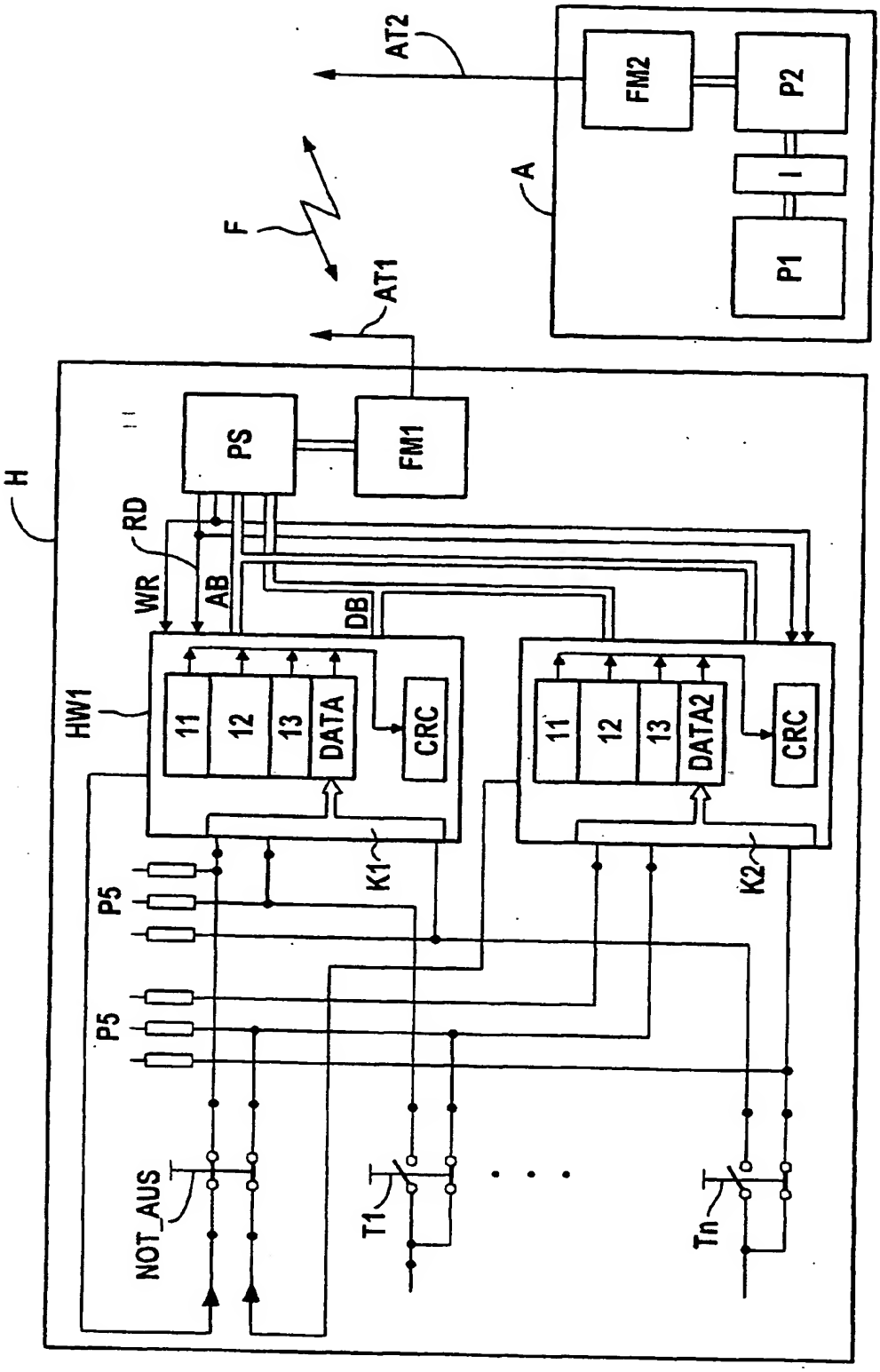


FIG 4